

UNITED STATES DISTRICT COURT  
DISTRICT OF MARYLAND

CHAMBERS OF  
CHARLES B. DAY  
UNITED STATES MAGISTRATE JUDGE

U.S. COURTHOUSE  
6500 CHERRYWOOD LANE  
GREENBELT, MARYLAND 20770  
(301) 344-0393  
FAX (301) 344-0394

May 17, 2010

**VIA ELECTRONIC FILING**

Stephen Howard Ring, Esquire  
Stephen H. Ring, P.C.  
506 Main Street, Suite 215  
Gaithersburg, Maryland 20878

Michael S. Rothman, Esquire  
Law Office of Michael S. Rothman  
401 E. Jefferson Street, Suite 201  
Rockville, Maryland 20850

Sanford M. Saunders, Jr., Esquire  
Nicoleta Burlacu, Esquire  
Greenberg Traurig  
2101 L Street, NW, Suite 1000  
Washington, DC 20037

John L. McManus, Esquire  
Kenneth A. Horky, Esquire  
Greenberg Traurig  
401 E Las Olas Boulevard, Suite 2000  
Fort Lauderdale, Florida 33301

Re: Beyond Systems, Inc. v. World Avenue USA, LLC.  
Civil Action No. PJM-08-921

Dear Counsel:

Pursuant to the referral of this case to me for resolution of discovery disputes, the Court has received Defendant World Avenue, USA, LLC's Sealed Motion to Challenge Plaintiff Beyond Systems, Inc.'s Designation of 68,300 Documents as Confidential and for Sanctions and Incorporated Memorandum of Law ("Defendant's Motion")(originally filed as Docket Item No. 119, and filed under seal as Docket Item No. 122). The Court has reviewed Defendant's Motion and memoranda related thereto. No hearing is deemed necessary. Local Rule 105.6 (D. Md.). The Court hereby GRANTS Defendant's Motion.

Defendant challenges Plaintiff's "designation of approximately 68,300 emails produced in discovery" as confidential under the Confidentiality Order entered in this case. Plaintiff has maintained that said emails were sent to it from Defendant in violation of laws regarding unsolicited commercial electronic mail ("UCE").

Without doubt, under federal law and the terms of the Confidentiality Order, the burden of establishing the confidentiality of materials rests upon the party seeking the designation.

It is correct that the burden of justifying the confidentiality of each and every document sought to be covered by a protective order remains on the party seeking the protective order; any other conclusion would turn Rule 26(c) on its head. That does not mean,

however, that the party seeking the protective order must necessarily demonstrate to the court in the first instance on a document-by-document basis that each item should be protected. It is equally consistent with the proper allocation of evidentiary burdens for the court to construct a broad “umbrella” protective order upon a threshold showing by one party (the movant) of good cause. Under this approach, the umbrella order would initially protect all documents that the producing party designated in good faith as confidential. After the documents are delivered under this umbrella order, the opposing party could indicate precisely which documents it believed to be not confidential, and the movant would have the burden of proof in justifying the protective order with respect to those documents. The burden of proof would be at all times on the movant; only the burden of raising the issue with respect to certain documents would shift to the other party.

Cipollone v. Liggett Group, Inc., 785 F.2d 1108, 1122 (3d Cir. 1986), cert. denied, 484 U.S. 976. See also Local Rule 104.13. This Court’s Confidentiality Order provides a generic “umbrella” of non-disclosure of Plaintiff’s documents in the absence of a specific challenge. Defendant has met its burden of “raising the issue” challenging the designation and Plaintiff must now provide the justification for continued confidentiality. Contrary to the suggestion of Plaintiff, the existence of a Confidentiality Order is neither an iron clad cloak of protection of the materials from non-disclosure, nor is it dispositive of Defendant’s Motion.

Plaintiff has designed its system to receive suspected unlawful electronic mail to inactive electronic mail addresses. Plaintiff’s main position is that “the confirmed, functioning recipient email addresses, contained within the headers” of the electronic mail merits protection. Plaintiff contends that allowing disclosure of these inactive addresses to the general public would make these addresses the target of additional unwanted electronic mail. Plaintiff claims that “verification of functioning email addresses renders them more valuable as targets for unsolicited commercial email (UCE).” Plaintiff also notes that redacting the headers of these emails is impractical, and doing so would have only marginal value. Finally, Plaintiff’s position is that its use of inactive addresses to identify UCE is consistent with industry practice and Plaintiff provides a declaration from an unrelated litigation in support of this position.

The problem with Plaintiff’s approach is that the UCE, and the address headers, were not created by Plaintiff, and are the gravamen of this litigation. Unlike the situation involving some true trade secret, the UCE at issue were not generated by Plaintiff, but by the allegedly offending party. Plaintiff’s complaint is merely that if the addresses of its “spam traps” are made public, it will be victim to more spam. Sad as it may be, this is an insufficient reason to justify the non-disclosure of these addresses.

The sole purpose of Plaintiff's spam trap is to use information sent there as an enforcement tool against suspected offenders. Plaintiff has no interest, of a confidential nature, in the substance of the messages. The addresses are public in the sense that they are not shielded from public view. Whether by automated means or otherwise, the addresses employed are in the public domain. The bar of confidentiality is a high one, reserved for the subjects of matters protected by privileges, "trade secret, or other confidential research, development, or commercial information." Fed. R. Civ. P. 26(b) and (c)(1)(G). Plaintiff's technique is neither a trade secret, nor confidential within the meaning of the Rules. Plaintiff is merely using inactive mail addresses to find out who is sending unwanted mail. The fact that Plaintiff uses the addresses as part of a "trap," is not a sufficient reason to keep the world from knowing what some are already equipped to find out. Simply put, the addresses that Plaintiff seeks to hide from view are already available to the general public. See Minter v. Wells Fargo Bank, N.A., 258 F.R.D. 118 (D. Md. 2009).

Defendant also astutely points out that of the 68,300 electronic mail messages, at best Plaintiff's argument relates to approximately 900. There is no justification for the continued designation of confidentiality to the overwhelming balance of messages, and Plaintiff's claim of burden for redactions is unpersuasive.

As the Court is granting Defendant's Motion, the 68,300 electronic mail messages are "de-designated" as confidential. Despite the informal nature of this letter, it is nonetheless an Order of the Court, and the Clerk is directed to docket it as such.

Very truly yours,

/s/

Charles B. Day  
United States Magistrate Judge

CBD/bab